



FortiClient (Mac OS X) - Release Notes

VERSION 5.4.1

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



July 7, 2016

FortiClient (Mac OS X) 5.4.1 Release Notes

04-541-357382-20160707

TABLE OF CONTENTS

Change Log	4
Introduction	5
Licensing	5
Standalone Mode	5
Managed Mode	5
Special Notices	7
SSL VPN Requirements	7
Cooperative Security Fabric Upgrade	7
Change in FortiClient Endpoint Control Default Registration Port	7
What's New in FortiClient (Mac OS X) 5.4.1	8
FortiClient Telemetry	8
Endpoint compliance	8
Installation Information	9
Firmware images and tools	9
Upgrading from previous FortiClient versions	9
Downgrade to previous versions	9
Uninstall FortiClient	9
Firmware image checksums	10
Product Integration and Support	11
FortiClient 5.4.1 support	11
Language support	11
Resolved Issues	13
Known Issues	14

Change Log

Date	Change Description
2016-07-06	Initial release.
2016-07-07	Added special notice about SSL VPN requirements.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Mac OS X) 5.4.1 build 0514.

This document includes the following sections:

- [Introduction](#)
- [Special Notices](#)
- [What's New in FortiClient \(Mac OS X\) 5.4.1](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

Please review all sections prior to installing FortiClient. For more information, see the *FortiClient Administration Guide* in the [Fortinet Document Library](#).

Licensing

FortiClient offers two licensing modes:

- Standalone Mode
- Managed Mode

Standalone Mode

In standalone mode, FortiClient is not registered to a FortiGate or Enterprise Management Server (EMS). In this mode, FortiClient is free both for private individuals and commercial businesses to use. No license is required.



Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed Mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can register to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

FortiClient Licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient Licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

SSL VPN Requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
This document is available on the Fortinet Document Library on the FortiOS page (docs.fortinet.com/).
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*
This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2 (support.fortinet.com/).

Change in FortiClient Endpoint Control Default Registration Port

FortiClient registers to the FortiGate using Endpoint Control (EC). In FortiClient 5.0 and 5.2, the default registration port is TCP port 8010. FortiOS 5.0 and 5.2 both listen on TCP port 8010.

Starting with FortiClient 5.4, EC registration will use port 8013 by default. To register to FortiOS 5.0 or 5.2, the user must specify port 8010 with the IP address, separated by a colon. For example, <ip_address>:8010.

FortiOS 5.4 and later will listen on port 8013. If registering from FortiClient 5.4 and later to FortiOS 5.4 and later, the default ports will match. Specifying the port number with the IP address is then optional.

What's New in FortiClient (Mac OS X) 5.4.1

This section identifies the new features and enhancements in FortiClient (Mac OS X) 5.4.1. For more information, see the *FortiClient Administration Guide*.

FortiClient Telemetry

FortiClient can send endpoint telemetry data to FortiGate or FortiClient Enterprise Management Server. Telemetry data can include user identity and endpoint security context, such as vulnerability, security posture, OS details, interface, IP address, and MAC address.

Endpoint compliance

FortiClient can detect unauthorized and vulnerable endpoints. It helps enforce minimum compliance criteria and only allow network access to compliant endpoints.

If you are using FortiGate, FortiOS 5.4.1 is required.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.1, you can choose the setup type that best suits your needs. You can select one of the following options:

- Complete: all Endpoint Security and VPN components will be installed.
- VPN Only: only VPN components (IPsec and SSL) will be installed.

FortiClient includes various tools to help with and customize installations. The following tools and files are available in the *FortiClientTools* file:

- *OnlineInstaller*: downloads and installs the latest FortiClient file from the public FortiGuard Distribution Server (FDS).
- *FortiClientConfigurator*: an installer repackaging tool that can be used to create custom installation packages
- *RebrandingResources*: resources used by the FortiClient Configurator tool for rebranding.



When creating a custom FortiClient 5.4.1 installer using the FortiClient Configurator tool, you can choose which features to install. You can also enable or disable software updates, configure SSO, and rebrand FortiClient .

Upgrading from previous FortiClient versions

FortiClient version 5.4.1 supports upgrading from FortiClient 5.2.0 or later.

When FortiClient endpoints are registered to FortiGate, you must upgrade endpoints to FortiClient 5.4.1 before you upgrade FortiGate to 5.4.1. See [Cooperative Security Fabric Upgrade on page 7](#).



Please review the following sections prior to installing FortiClient version 5.4.1: [Introduction on page 5](#), [Special Notices on page 7](#), and [Product Integration and Support on page 11](#).

Downgrade to previous versions

Downgrading FortiClient version 5.4.1 to previous FortiClient versions is not supported.

Uninstall FortiClient

To uninstall FortiClient version 5.4.1, use the *Application > FortiClient > Uninstaller* application.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at <https://support.fortinet.com>. After logging in, click on *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 5.4.1 support

The following table lists FortiClient (Mac OS X) 5.4.1 product integration and support information.

Desktop Operating Systems	<ul style="list-style-type: none">• Mac OS X v10.8 Mountain Lion• Mac OS X v10.9 Mavericks• Mac OS X v10.10 Yosemite• Mac OS X v10.11 El Capitan
Minimum System Requirements	<ul style="list-style-type: none">• Intel processor• 256MB of RAM• 20MB of hard disk drive (HDD) space• TCP/IP communication protocol• Ethernet NIC for network connections• Wireless adapter for wireless network connections• Adobe Acrobat Reader for FortiClient documentation
FortiAnalyzer	<ul style="list-style-type: none">• 5.4.1
FortiAuthenticator	<ul style="list-style-type: none">• 4.1.0• 4.0.0 and later• 3.3.0 and later• 3.2.0 and later• 3.1.0 and later• 3.0.0 and later
FortiClient EMS	<ul style="list-style-type: none">• 1.0.0 and later
FortiManager	<ul style="list-style-type: none">• 5.4.1
FortiOS	<ul style="list-style-type: none">• 5.4.1 <p>Some FortiClient features are dependent on specific FortiOS versions.</p>

Language support

The following table lists FortiClient language support information.

Language	GUI	XML Configuration	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓		
Chinese (Traditional)	✓		
French (France)	✓		
German	✓		
Japanese	✓		
Korean	✓		
Portuguese (Brazil)	✓		
Russian	✓		
Spanish (Spain)	✓		

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.



If the client workstation is configured to a regional language setting that is not supported by FortiClient , it defaults to English.

Resolved Issues

The following issues have been fixed in FortiClient (Mac OS X) 5.4.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
291465	Software update is displayed even when disabled.
294213	DNS traffic may stop working with SSL VPN split tunnel on Mac OS X 10.11.
298065	FortiClient may cause random system crashes and reboots on Mac OS X El-Capitan.
309575	Network traffic may stop working after IPsec VPN connection is established.
374531	FortiClient Mac shows wrong on-net off-net status.
375140	SSL VPN does not auto-connect after disconnect or reboot.
373501	SSL VPN user certificate selection not preserved.
374006	SSL VPN does not work with multi-factor authentication.
354650	NetBIOS lookup fails when connected to SSL VPN.
368399	Cannot assign manual IPsec virtual IP from config.
365722	SSL VPN does not support multiple DNS suffix.
356782	Right-click FortiClient Tray icon to connect to VPN produces another prompt window.
309575	IPSec issue on Mac 10.11 El Capitan.
294213	SSL VPN DNS issue on Mac 10.11 El Capitan.

Known Issues

The following issues have been identified in FortiClient (Mac OS X) 5.4.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
271427	Host CPU may increase when using the <code>type ahead</code> feature in Eclipse Luna on Mac OS when FortiClient is registered on FortiGate.



FORTINET®

High Performance Network Security



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.